Collins Aerospace

INTEGRATION OF SEL4 IN A FLIGHT VEHICLE MISSION SYSTEM

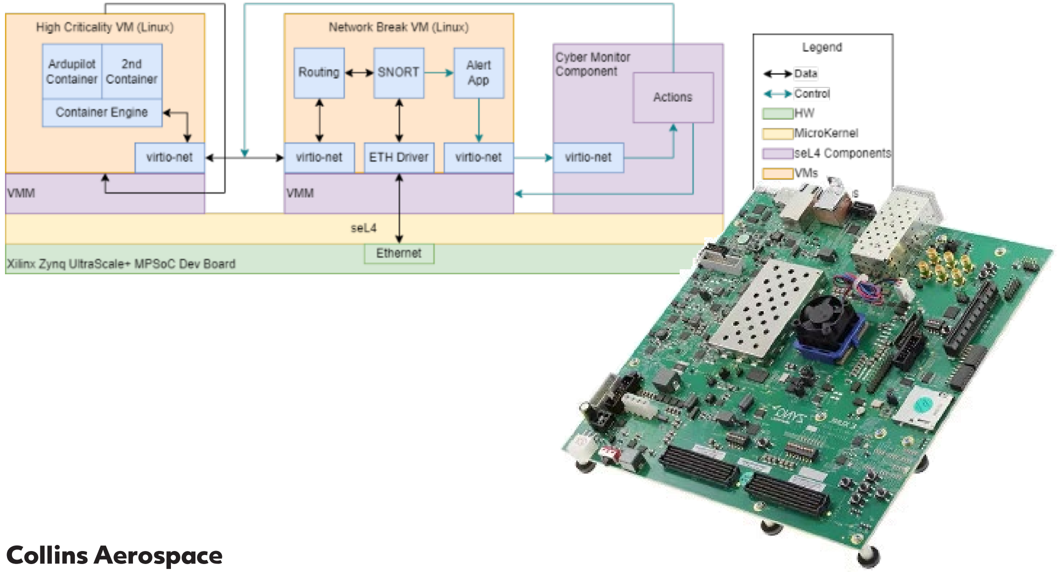
Darren Cofer

5 Sept 2025

TA2 PLATFORM DEVELOPMENT

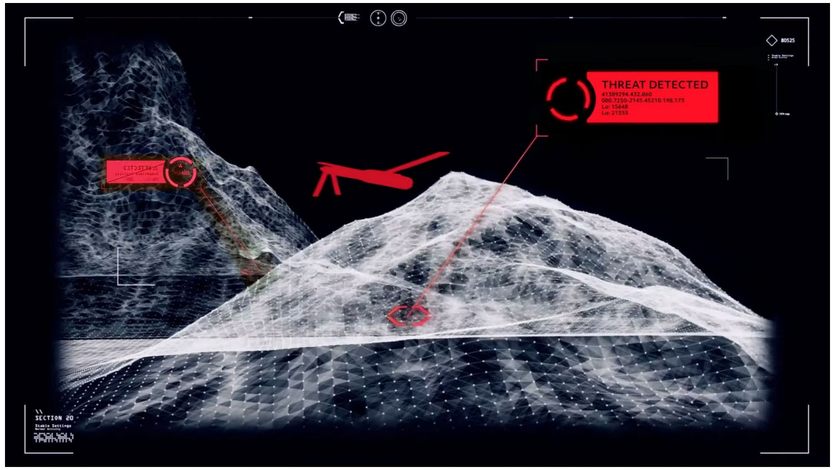
OPEN PLATFORM

- Developed and supported by DornerWorks
- Unrestricted UAV mission software (based on ardupilot), system model with formal properties, multiple VMs, Rust software components, seL4 kernel
- Xilinx Zynq UltraScale+ MPSoC-based development board



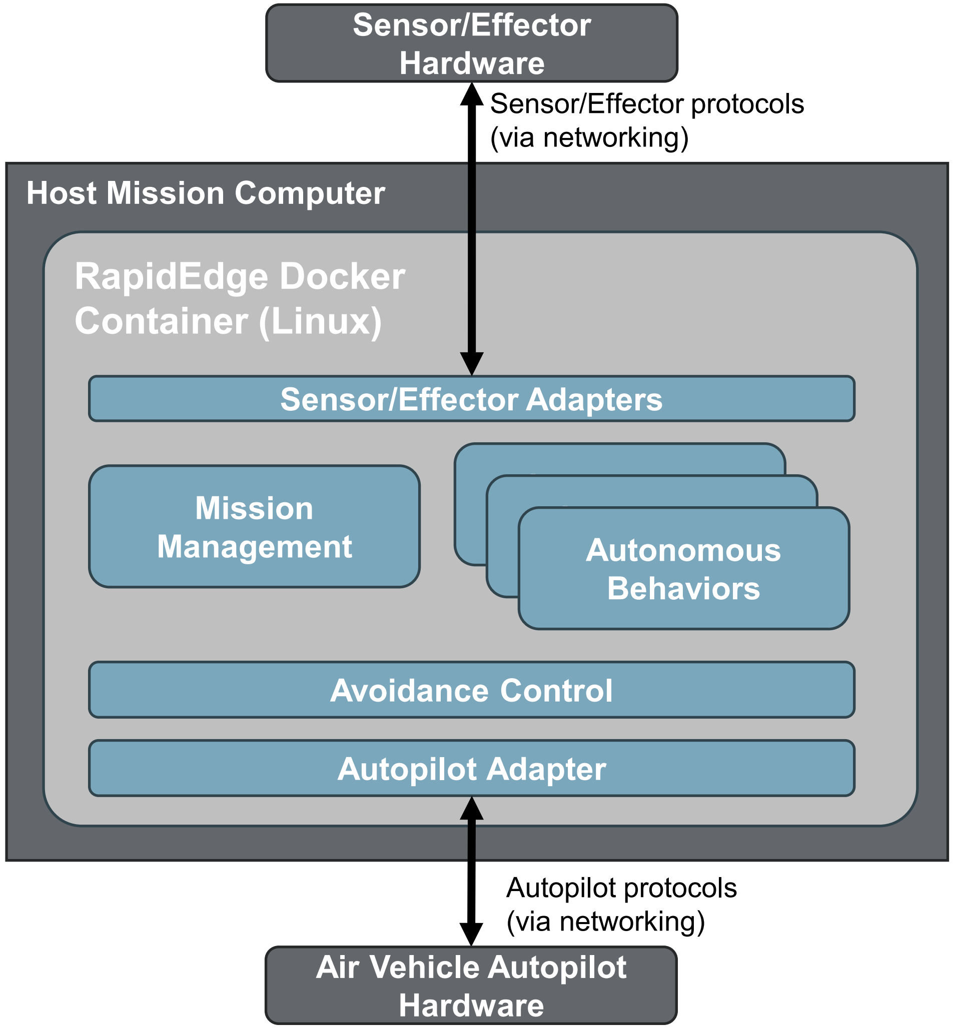
RESTRICTED PLATFORM

- Collins RapidEdge™ technology provides mission computing for collaborative autonomy, interfacing with onboard sensors and radios and handling multiple levels of classified data
- Deployable in small unmanned air vehicles with the ability support a variety of payloads
- Based on same computing hardware family as Open Platform



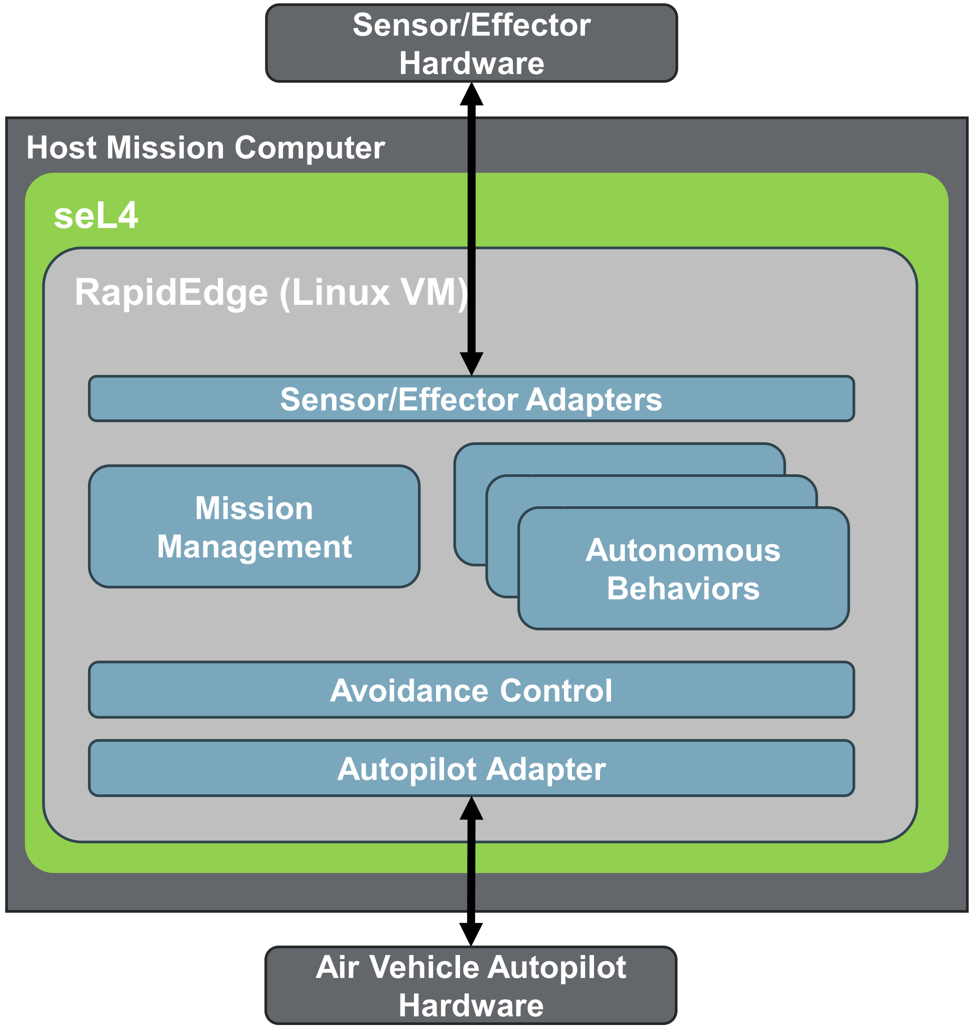
Collins Aerospace

RAPIDEDGE MISSION SOFTWARE



- Based on MOSA (Modular Open Systems Approach) architecture
  - Standardized interfaces for seamless integration
  - Scalable, vendor-agnostic architecture
  - Supports future tech upgrades with minimal changes
- Deployment via Linux container
  - Can run directly without containerization; very light on dependencies
- Interfaces to the outside world (sensors and flight control) are via network (IP)
- x86-64 and aarch64 supported
  - Most current deployments are based on Zynq UltraScale+ MPSoC hardware
  - Same as open platform

MISSION SYSTEM DEMO ON SEL4



- The PROVERS INSPECTA team has completed our initial integration of the seL4 formally verified secure kernel with RapidEdge mission system software
- The integrated software was able to successfully execute in hardware-in-the-loop simulation an autonomous multi-UAV surveillance mission
- The RapidEdge™ Collaborative Mission Autonomy software was run without modification in a secure virtual machine hosted on seL4, providing guaranteed isolation and control over all input and output interfaces
- This successful integration and demo provide the basis for further application of formal methods technologies in the coming phases of the PROVERS program and will result in verified cyber-resilience for the future UAV mission computing systems

Collins Aerospace

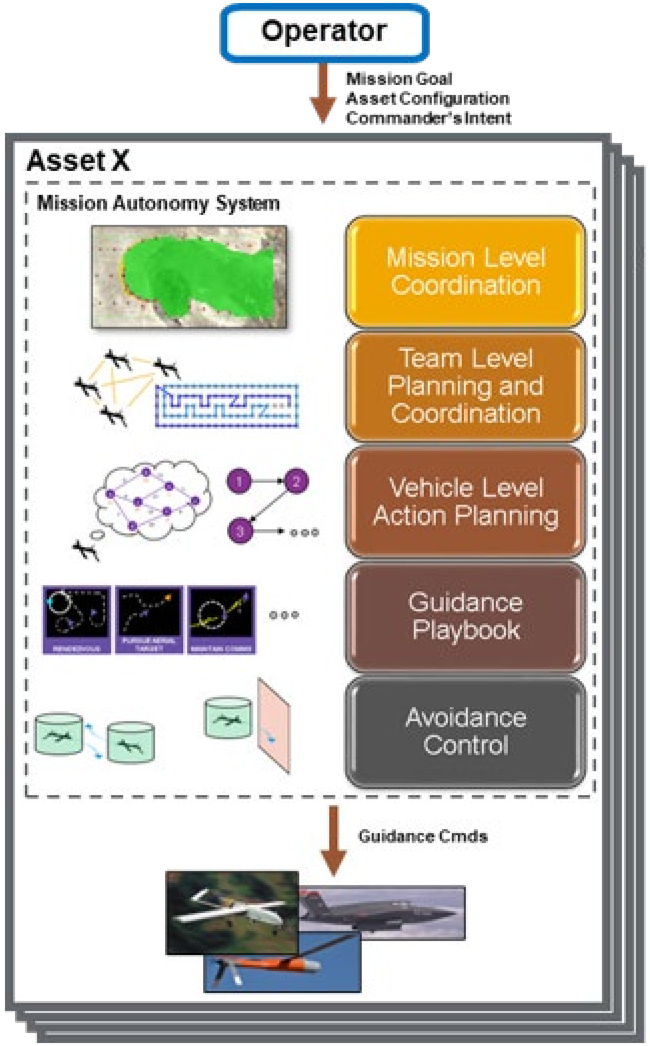
CHALLENGES AND SIMPLIFICATIONS

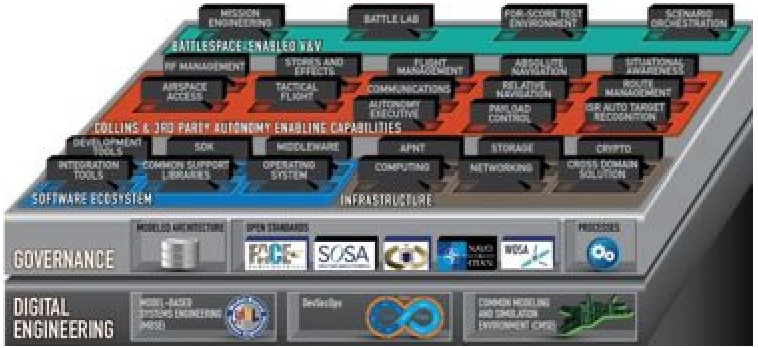
Challenge	Approach
Flight hardware expected to change in near future	Target ZCU-102 for demo (same MPSoC), port to new flight hardware when available
RapidEdge software requires utilization of multiple CPU cores to achieve desired performance	Split into two separate VMs and host on separate cores – straightforward because of RapidEdge architecture and networking
seL4 multicore/multi-kernel support still under development	Host one VM on seL4 now with others in SIL, update as multi-kernel support becomes available

Demonstrate initial RapidEdge/seL4 integration as soon as possible with incremental updates for new features

RapidEdge™ Mission Autonomy

- RapidEdge™ is the Collins branding for a suite of **autonomy-enabling edge capabilities**, along with the **reference architectures**, **integration/demonstration environments**, and **DevSecOps**/governance processes to enable rapid evolution from TRL 0-7
- The RapidEdge™ Mission Autonomy Suite is a **hierarchical** autonomy framework for **multi-vehicle autonomous mission execution** with minimal operator intervention:
  - Operator specifies high level mission goal, asset configuration, and "commander's intent" (e.g., mission preferences)
  - Software outputs guidance commands (e.g., airspeed, bank, vert speed) to dynamically steer the vehicle
  - In between, autonomy performs decentralized yet coordinated decision making, synchronization, team and individual level action planning, and automated absolute and relative guidance using common software on each platform
- The architecture and its components are modular and can be deployed either as:
  - A **wholesale autonomy engine**, or
  - A modular set of **autonomy-enabling components**

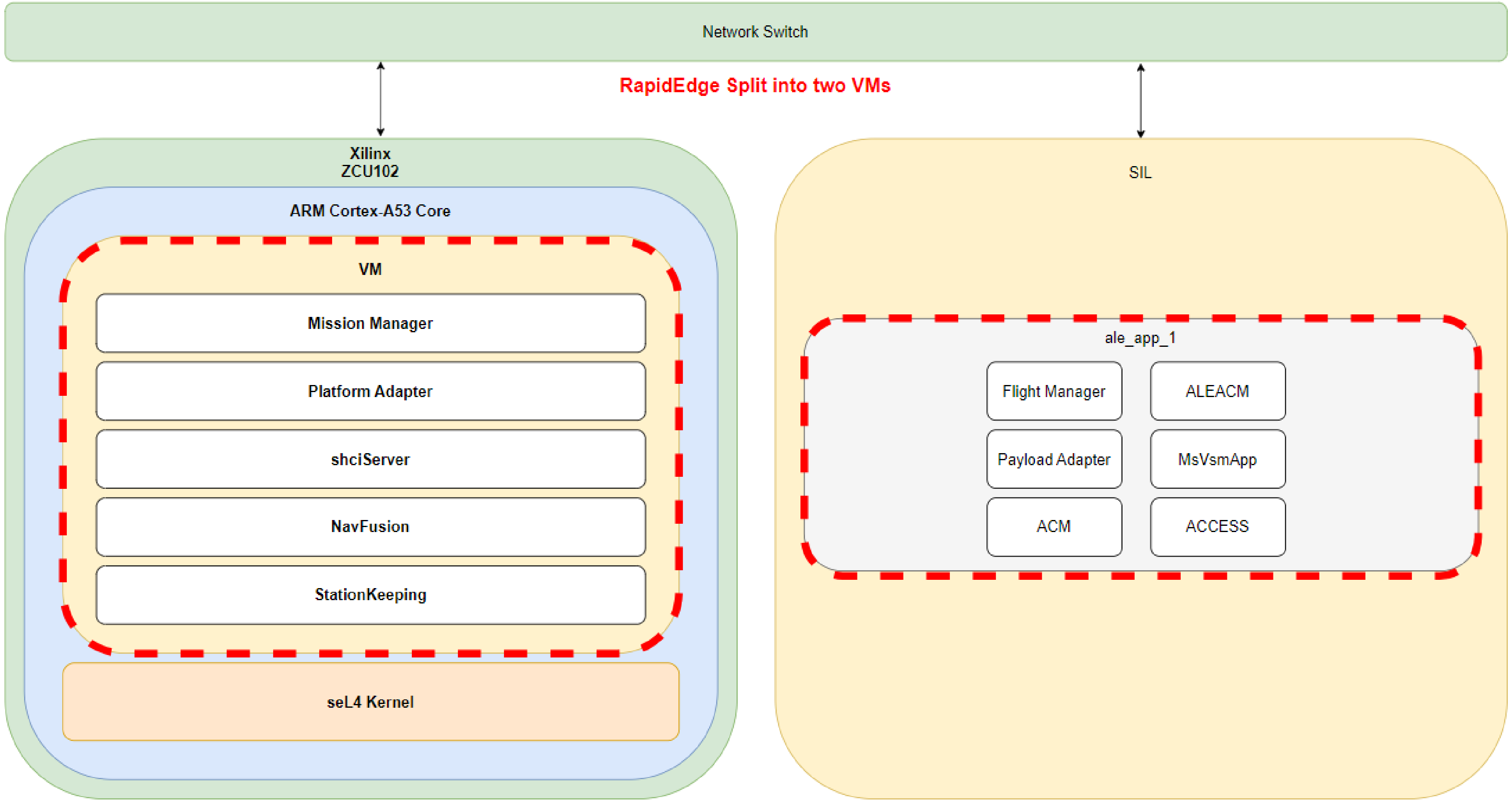




Autonomy Defined
- Umbrella term generally understood as a ***"system's ability to self-direct in an adaptive manner"***.
- In UAS space, typically aligned to:
  - Extending the reach, sensing, and lethality of platforms
  - Protecting high value assets
  - Elevating the operator-to-UAS relationship from 1-to-1 to 1-to-many

Collins Aerospace

DEMO CONFIGURATION

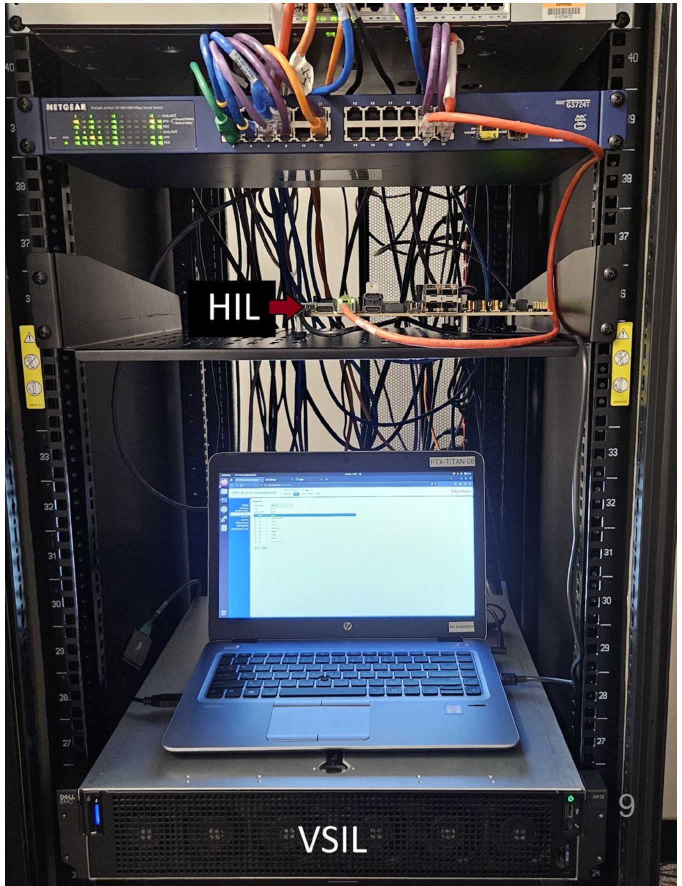


Collins Aerospace

VIRTUAL SYSTEM INTEGRATION LAB(VSIL) AND HARDWARE IN THE LOOP (HIL)

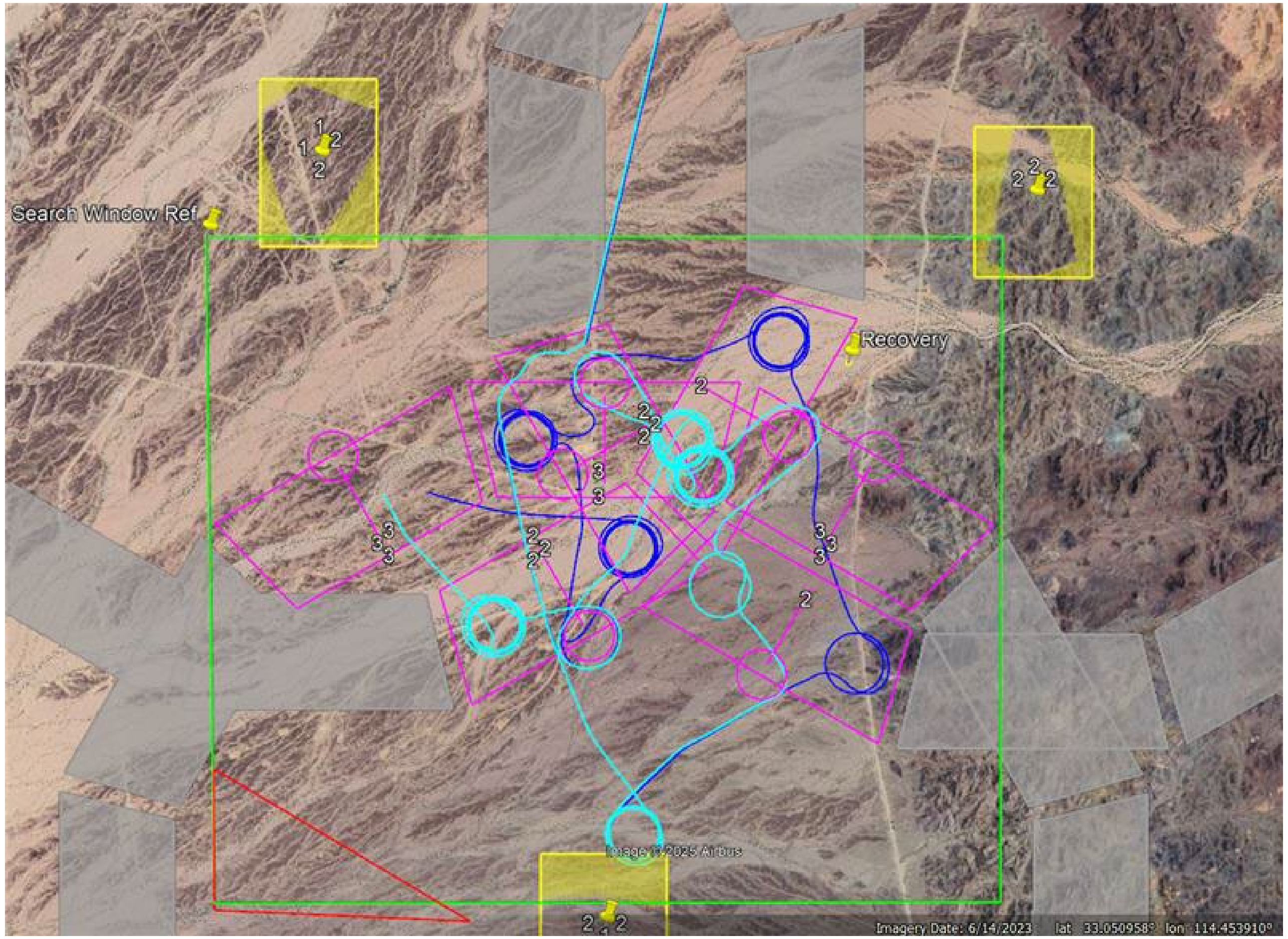
- The Xilinx ZCU102 used as the target hardware component for this demonstration in the HIL
- The HIL is networked to the VSIL with a Sim Support software in the loop (SIL)
- The HIL is running the RapidEdge™ autonomy software in a virtual machine on top of the seL4 microkernel
- The VSIL emulates all components of the flight system, that are not being run on the HIL
  - Air Vehicle performance Simulation
  - Payload Simulation
  - Two RapidEdge applications that don’t fit on single core

Xilinx ZCU102

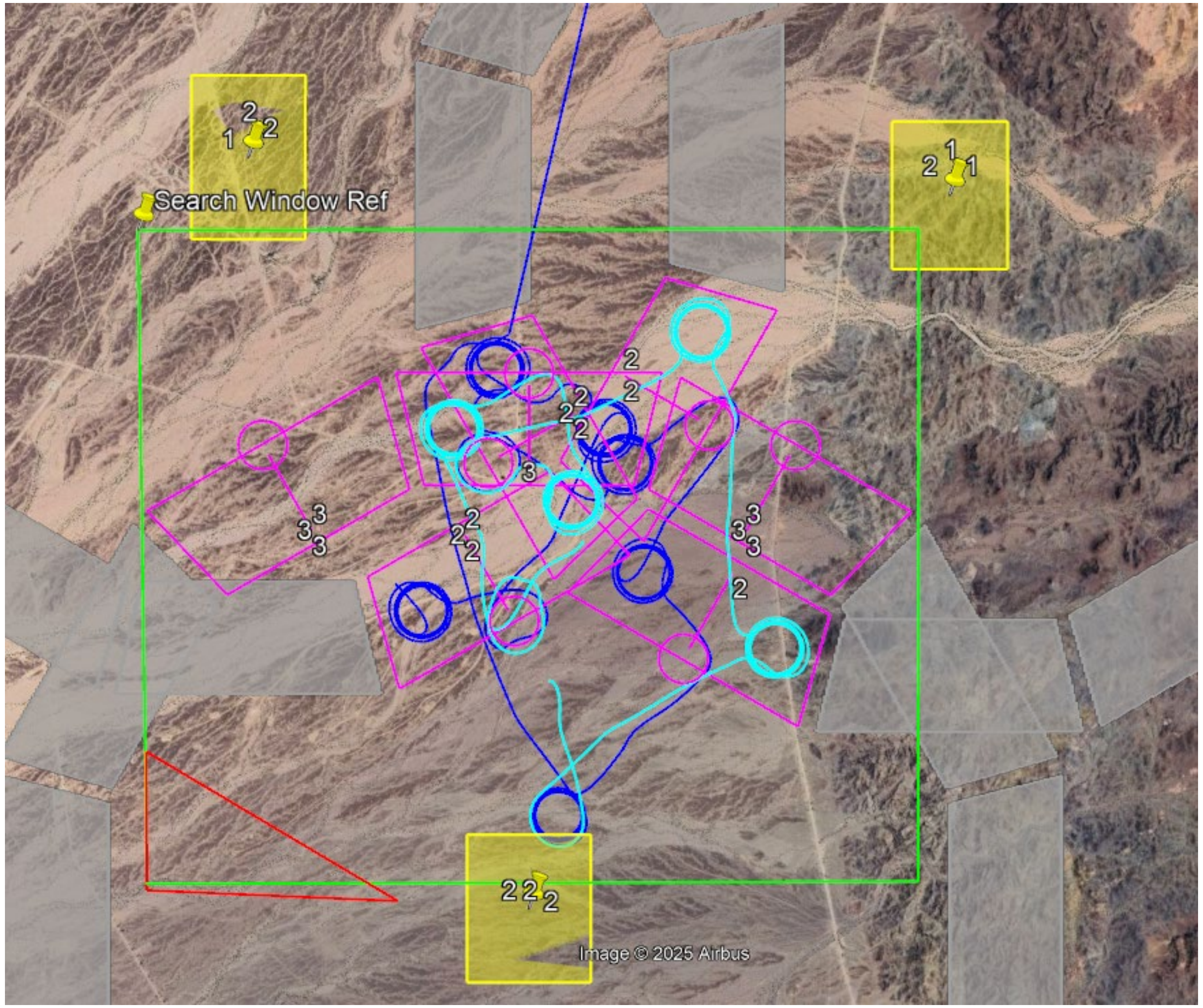


Collins Aerospace

SIDE BY SIDE WITH THE EXPECTED



Expected Flight Result



seL4 Solution

Collins Aerospace

SECURITY BENEFITS OF INITIAL INTEGRATION

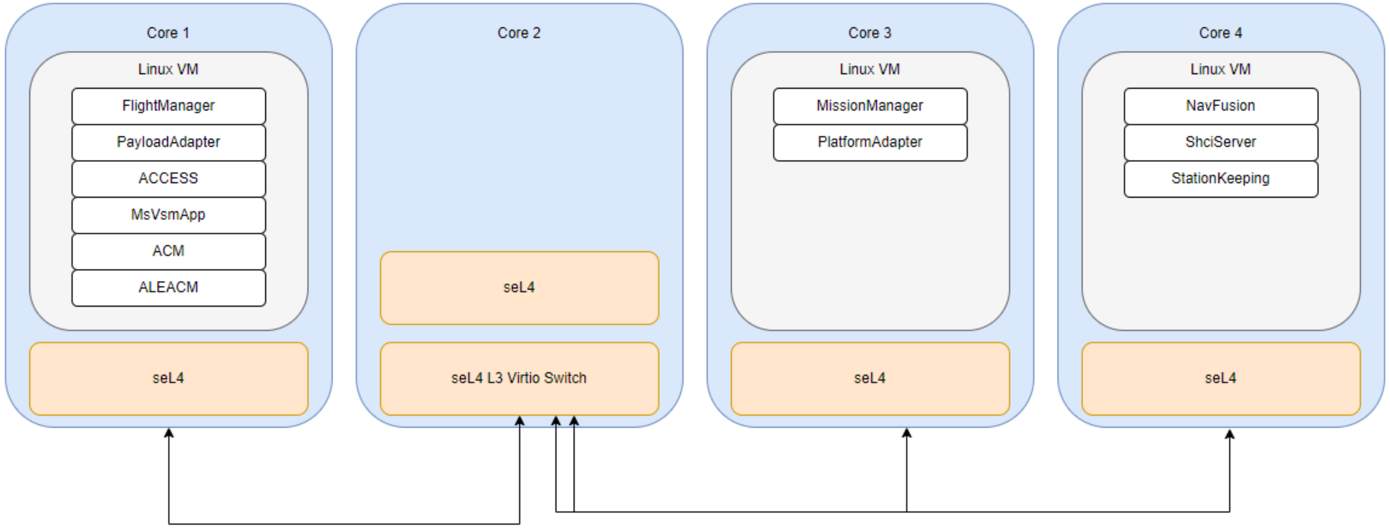
- Reduced Attack Surface with seL4
  - Minimal kernel with formally verified correctness
  - Exposed very few interfaces (one) reducing possible entry points for attackers
  - Similar to Open Platform use case
- Formal verification of seL4 provides proven security
- Strong Isolation between VMs and Components
  - Isolation of the VM is enforced at the kernel level
  - VMs and components can’t access resources they aren’t explicitly granted
- Allows for enhanced security without change to existing source code

Collins Aerospace

NEXT STEPS

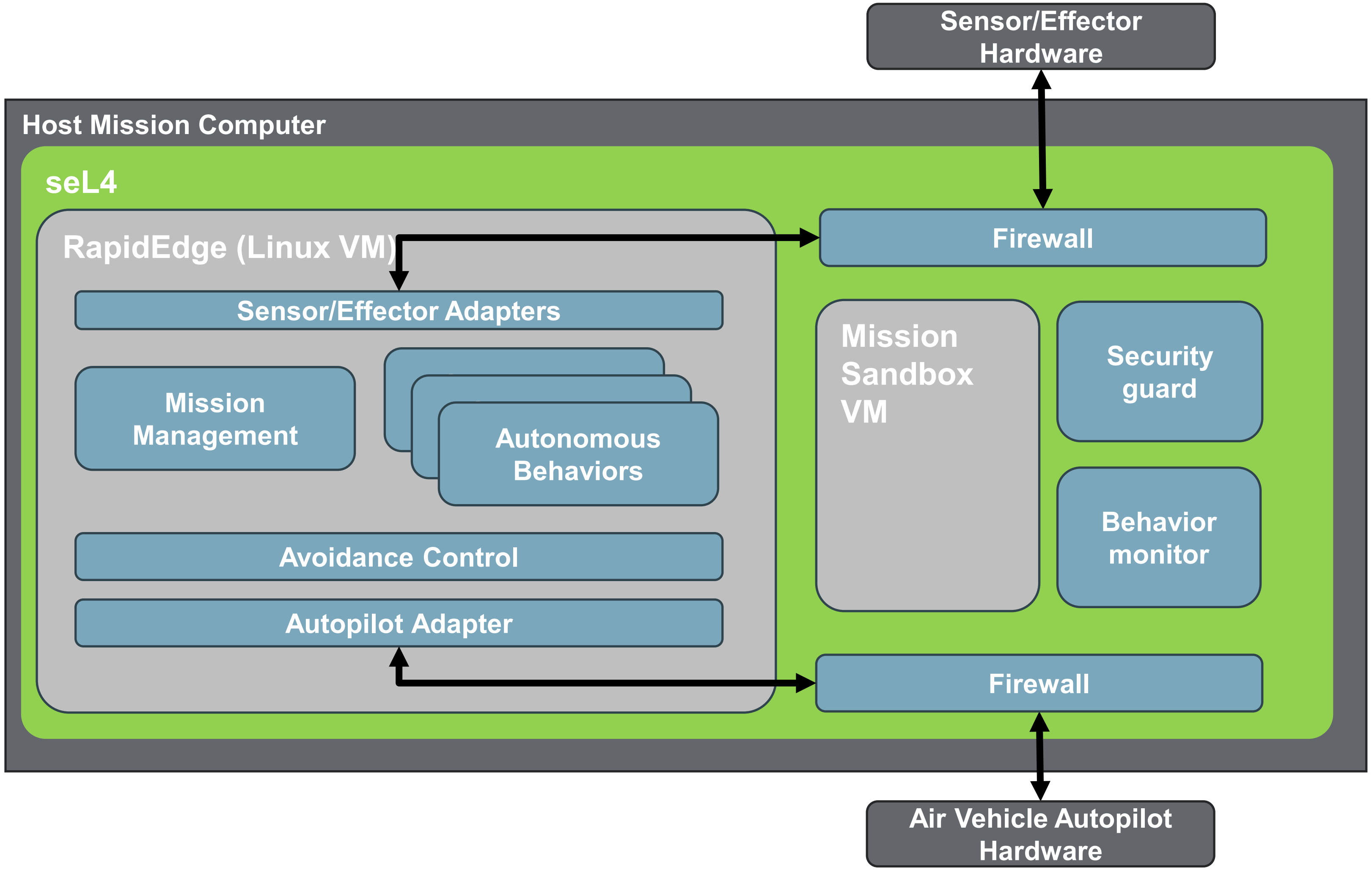
Phase 2 & 3 improvements:

- Multi-kernel support
- Single vs. multiple VMs
- seL4 microKit vs. CAmkES
- Move from ZCU102 to VNX Racerunner hardware
- INSPECTA tool support for analysis and build process



Collins Aerospace

NEXT STEPS

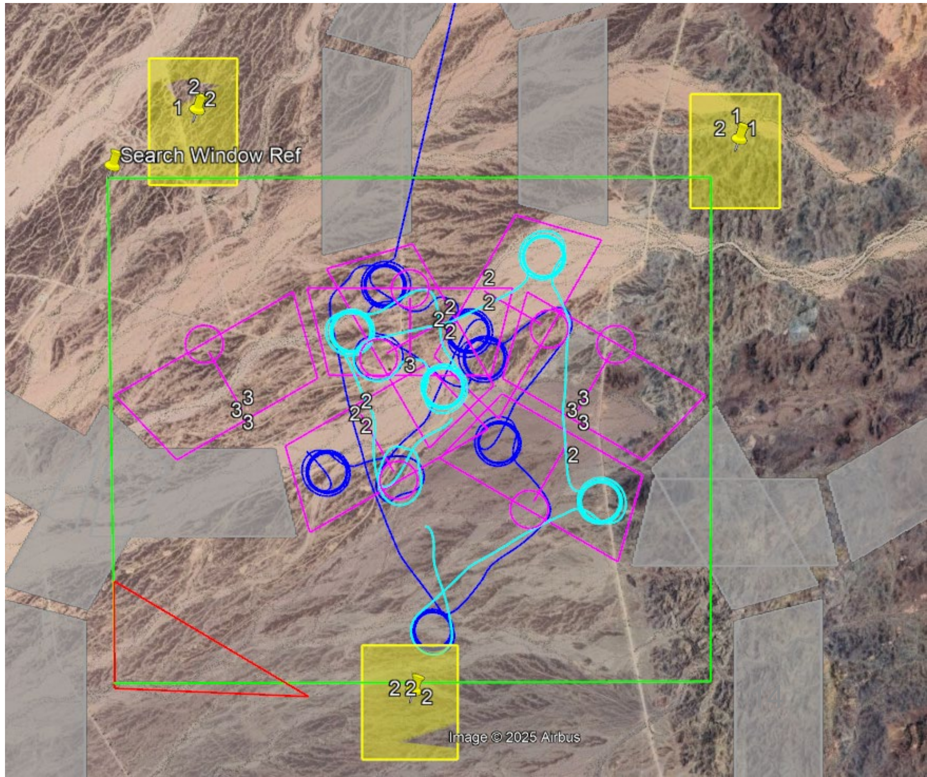


Advanced features

- New cybersecurity features
  - Firewall
  - Network guard
  - File system check
  - Crypto services
  - Behavior monitor
- Sandbox VM
  - Support for rapid secure authority to operate (ATO) and deployment of new functionality

CONCLUSION

- Successfully integrated the RapidEdge autonomy into a seL4 environment
- Verified that software works as expected in hardware-in-the-loop simulation
- Showed the same flight behavior in this sim that was seen in flight demo
- Positioned the team for progress on future goals
  – seL4 multicore/multi-kernel solution
  – Transition to new flight hardware
  – Advanced cybersecurity features
  – Demo of INSPECTA tool pipeline



Collins Aerospace